IN THE UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

SUMMIT 360, INC.,	)	
	)	
Plaintiff,	)	
v.	)	Case No. 0:25-CV-02202
	)	
CISCO SYSTEMS, INC.,	)	
	)	**JURY TRIAL DEMANDED**
Defendant.	)	

COMPLAINT

Plaintiff Summit 360, Inc. ("Summit 360"), by its undersigned attorneys, brings this Complaint against Defendant Cisco Systems, Inc. ("Cisco") and hereby alleges as follows:

INTRODUCTION

1. Cisco is a quintessential monopolist. Almost forty years ago, Cisco successfully commercialized the concept of computer networking and, since then, has enjoyed a dominant share of the networking market in both the United States and globally. To expand its footprint, Cisco has engaged in serial acquisitions of competitors and other companies, whose innovations Cisco could not muster itself. Today, Cisco is not a monopolist because of its ingenuity or vision; on the contrary, Cisco is a monopolist because of its abuse of market power to limit the ability of networking competitors to meaningfully challenge it and the ability of networking customers to discipline it. Because Cisco willfully maintains its

monopolies through anticompetitive conduct, Summit 360 brings this lawsuit to put an end to Cisco's anticompetitive schemes.

2. For almost four decades, Cisco has sat atop this multi-billion-dollar industry—an industry where Cisco enjoys greater than 50 percent of the market share and little meaningful competition. Given its early market entrance and dominance, Cisco has become synonymous with computer networking. In today's modern workplace, computer networking is essential for any business to function and is utilized in businesses of all shapes and sizes—from airlines, to school districts, to law firms, and publicly traded companies. Computer networking serves a critical function for businesses to access and share data across the Internet and other networks. For businesses and governmental agencies large and small, networking equipment is a significant expense, and substituting equipment from one networking manufacturer to another is cost prohibitive. As an industry pioneer, Cisco has enjoyed a market-leading installed base and, with its dominant market power, has been able to maintain supra-competitive prices on its equipment. Those supra-competitive prices are often far too expensive for the average American business.

3. To maintain control over this market, Cisco has engaged in a systemic anticompetitive scheme designed to eliminate independent networking equipment resellers, like Summit 360 (the "Independent Channel"), who can offer

equipment that fits customer needs and budgets. The Independent Channel directly competes with Cisco's army of contract resellers and sales representatives (the "Authorized Channel"), who are incentivized to promote Cisco's interests. In short, the Independent Channel cuts into Cisco's multi-billion-dollar market. In response, Cisco has effectively sought to eradicate an entire market that offers more affordable options to end-users through a series of coercive and deceptive practices, as well as through the establishment and maintenance of technological barriers to entry to forestall the Independent Channel's ability to continue to compete with Cisco's Authorized Channel.

4. Cisco's go-to anticompetitive tactics, institutionalized within the company, include the use of fear, uncertainty, and doubt (or "FUD")—a term that Cisco and its employees have frequently used—towards its own customers and their purchase of any product or service through channels that Cisco does not approve, like the Independent Channel. Such FUD tactics have involved threats and intimidation to coerce customers into purchasing exclusively through Cisco's Authorized Channel of resellers and not through other channels independent of Cisco. Cisco's sales representatives have even threatened to suspend and/or terminate services already paid for by customers if they purchased networking equipment from the Independent Channel. This is a powerful threat because of Cisco's near-virtual monopoly in service. Cisco has made good on its threats if a

customer makes the "wrong" choice. In the last seven years, two federal courts have held that there was sufficient evidence to find that Cisco is a monopolist who has abused its market power to maintain or enhance its monopolies—using anticompetitive tactics like FUD—in violation of the Sherman Act.

5. More recently, Cisco has taken advantage of its licensing agreements and rights to further steer end-users away from purchasing hardware through the Independent Channel. As with most modern equipment, Cisco embeds software within its networking equipment and requires end-users to execute licensing agreements to use the equipment. In doing so, Cisco leverages its rights as a licensor against end-users that it suspects and/or knows to have purchased equipment from independent resellers, to force them to cease purchasing equipment from the Independent Channel. Indeed, Cisco has not hesitated to threaten to conduct audits or impose fines against its end-users or to demand written commitments that they will no longer purchase from the Independent Channel.

6. Cisco has also rolled out a new fleet of networking equipment that further restricts access to updates to its internetwork operating system ("IOS")—which are critical to modern-day switches and routers—to *only* customers who purchased hardware through the Authorized Channel. In doing so, Cisco effectively deprives Independent Channel purchasers of essential updates. But

this is all by design: by restricting access to updates only to the Authorized Channel, Cisco is exploiting its end-users, who are locked-in to Cisco, and forcing them to leave the Independent Channel in favor of the Authorized Channel.

7. There is no legitimate business justification for Cisco's exploitative practices. These tactics, on the contrary, are intentionally calculated to maintain Cisco's market power and control of the networking industry and to address Cisco's primary target, the Independent Channel, which Cisco has determined presents a top threat to its ability to charge supra-competitive prices to its customers. The Independent Channel serves an important market need for customers by fulfilling their orders quicker than Cisco and at far lower prices, which fit within the limited budgets of our country's small businesses and institutions. One such independent reseller is Summit 360, a Minnesota-based networking equipment supplier, who has been in business for more than thirty years and sells a variety of networking products from Cisco and Cisco competitors.

8. True to form, Cisco has employed various FUD tactics against Summit 360's customers, including, among other things, (i) casting fear, uncertainty, and doubt as to the equipment Summit 360 supplies; (ii) threatening to conduct internal audits of customer networks; and (iii) imposing penalties for not using a reseller of Cisco's choosing. In one example, a Cisco sales representative misled a Summit 360 customer—without any proof—into believing

that Summit 360 sold it counterfeit products. When confronted by the customer, Cisco later admitted its deception. Cisco's threats are not designed to protect any legal rights, but rather they are explicitly designed to limit customer choice, harm the competitive process, and maintain Cisco's monopolies.

9. Summit 360 brings this antitrust case because it has had enough. Most recently, Cisco demanded that Summit 360 essentially conduct an audit of its own business, pressing Summit 360 to divulge details of its inventory, sales, and business operations, even though there is no contractual relationship between the parties. Nevertheless, Summit 360 complied and provided information to Cisco, which reflected that Summit 360 acquired the products at issue from trusted sources, including from public school districts. Still not satisfied, Cisco demanded more information regarding Summit 360's sales records pertaining to Cisco-branded equipment. If Summit 360 refused, Cisco threatened to use its extensive resources to bring an intellectual property ("IP") lawsuit against Summit 360.

10. While Cisco demanded information from Summit 360, and Summit 360 was cooperating with Cisco in good faith, Cisco (or one of its authorized resellers) approached one of Summit 360's customers to dissuade it from making further purchases through the Independent Channel. Specifically, the Cisco representative told Summit 360's customer that the reseller was "under investigation"—as if Cisco were some type of law enforcement authority. This

scenario confirms that Cisco continues to use FUD tactics that—to use Cisco's own words—are "not pretty, but it works."

11. Summit 360 seeks for this Court to bring an end to this abusive use of monopoly power that has terrorized an entire industry and to hold Cisco accountable. Cisco's anticompetitive conduct violates Section 2 of the Sherman Act, 15 U.S.C. § 2, and the Minnesota Antitrust Law, Minn. Stat. §§ 325D.49 to 325D.66, and should be enjoined. This conduct includes Cisco's use of FUD tactics, audits, technological barriers, and threat of litigation against Summit 360. The latter is not immunized by the *Noerr Pennington* doctrine because, as at least one federal court has held, Cisco's legal threats are connected to its coercive anticompetitive conduct against customers and thus are part of the same anticompetitive scheme. In addition, Cisco's threats of an IP case are made in bad faith because Cisco is fully aware of its own counterfeiting problem and uses it for commercial gain. Should Cisco bring its threatened claims as counterclaims, Summit 360 will illustrate why Cisco should be enjoined from continuing this bad-faith and anticompetitive strategy.

THE PARTIES

12. Plaintiff Summit 360, Inc. is a Minnesota corporation with its principal place of business at 1060 Lone Oak Road, Suite 140, Eagan, Minnesota 55121.

13. Defendant Cisco Systems, Inc. is a Delaware corporation with its principal place of business at 170 W. Tasman Drive, San Jose, California 95134. According to Cisco's latest Form 10-K with the Securities and Exchange Commission, its 2024 total U.S. revenue was $31.9 billion ($53.8 billion globally), with a reported gross margin of $21.4 billion ($36.3 billion globally).[1]

JURISDICTION

14. Summit 360 brings this case under Section 4 of the Clayton Act, 15 U.S.C. § 15, to recover treble damages, costs, and attorneys' fees for injuries sustained by Summit 360 because of Cisco's violation of Section 2 of the Sherman Act, 15 U.S.C. § 2.

15. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331, 1337, 1367(a), and Sections 4 and 16 of the Clayton Act, 15 U.S.C. §§ 15(a) and 26.

16. This Court also has jurisdiction pursuant to 28 U.S.C. § 1332. There is complete diversity of citizenship between Summit 360 and Cisco, and the amount in controversy exceeds seventy-five thousand dollars ($75,000.00), exclusive of interest and costs.

17. This Court has personal jurisdiction over Cisco because, *inter alia*, Cisco (i) transacted business throughout the United States, including in

[1] *See* Cisco Systems, Inc., *SEC Form 10-K*, 55, 102 (Sept. 5, 2024).

Minnesota, (ii) Cisco is registered to do business in Minnesota, (iii) Cisco provides routing and switching products throughout the United States, including in Minnesota, (iv) Cisco had sufficient minimum contacts with the United States, including Minnesota, and (v) Cisco engaged in anticompetitive conduct that was directed at and had a direct, foreseeable and intended effect of causing injury to the business or property of persons residing in, located in, or doing business throughout the United States, including in this District. In addition, this Court separately has personal jurisdiction over Cisco pursuant to Minn. Stat. § 542.09, because Cisco has engaged in wrongful conduct causing injury to Summit 360 in Minnesota.

18. Venue is appropriate in this district under Sections 4 and 12 of the Clayton Act, 15 U.S.C. §§ 15 and 22, and 28 U.S.C. §§ 1391(b), (c), and (d) because Cisco transacts business in this District and has served numerous customers within this District that utilize networking equipment.

FACTUAL BACKGROUND

19. Cisco is the largest manufacturer of switches and routers in the United States and worldwide. For Fiscal Year 2024, Cisco reported total U.S. revenue of approximately $30 billion in just core networking products.[2] At all relevant times in the Complaint, Cisco possessed a monopoly and market power

[2] *See* Cisco Systems, Inc., *SEC Form 10-K*, 39, 102 (Sept. 5, 2024).

in several markets related to networking equipment and services for the Internet. Cisco's core networking equipment monopolies are in routing and switching.

I. THE COMPUTER NETWORKING INDUSTRY

A. Cisco's Emergence as a Global Leader in The Computer Networking Industry.

20. Computer networking refers to the concept of connecting various computing devices (*i.e.*, laptops, smartphones, servers) to communicate with one another and exchange data. These devices are connected by both wired and wireless network solutions—such as local-area networks ("LANs") and wide-area networks ("WANs"). A typical networking architecture will have both switches and routers, which, as discussed further below, are essential products that enable computing devices to connect and exchange data.

21. In the mid-1980s and early-1990s, Cisco successfully commercialized the concept of computer networking, which coincided with the rise of the Dot-Com era. Specifically, Cisco developed networking hardware—namely switches and routers—that was capable of connecting computers at a distance. These early developments in computer networking played a key role in the development of the Internet. At the height of the Dot-Com era, Cisco reached a peak market capitalization of $500 billion—making it, at the time, the world's most valuable company.

B. Ethernet Switches and Networking Routers.

22. Ethernet switches are devices that control data flow within a network to enable network components to communicate efficiently. They are a fundamental building block to the modern LAN and WAN, and are deployed in virtually every networking environment, regardless of business. While Ethernet switches vary across vendors and customer types, there is no adequate substitute technology that provides the same function and value within a network infrastructure.

23. Routers are complementary products to Ethernet switches and are essential to any network architecture. While Ethernet switches connect computer components and devices to create a network, routers connect multiple switches and allow for communication between networks. As illustrated in Figure 1 below, these two devices generally operate at different logical levels in a network: Ethernet switches transfer information in the data link layer using physical addresses for network components, whereas routers (as the name suggests) "route" data from one network to another and control the flow of data traffic.

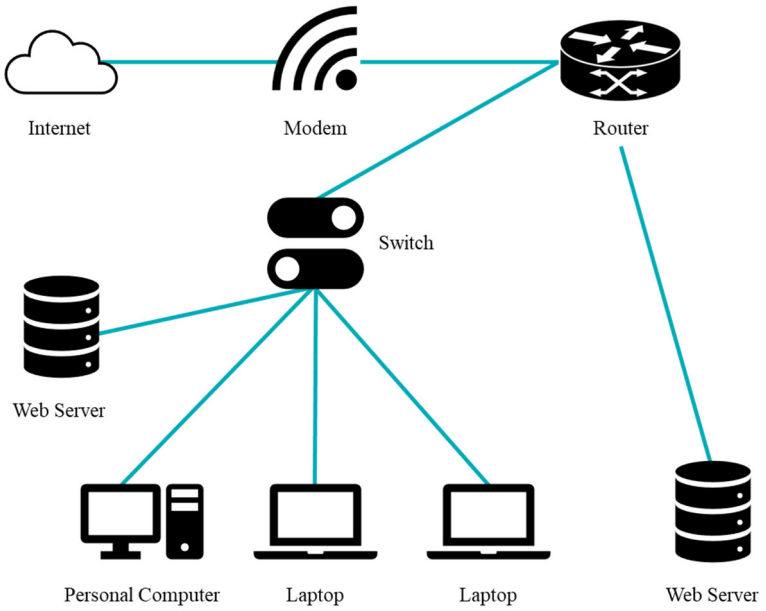

Figure 1

24. As technology has evolved, Ethernet switch manufacturers have begun to incorporate certain routing technologies into a single combined product, which further demonstrates that routers are complements for Ethernet switches and not substitutes.

25. Both Ethernet switches and routers are durable, high-fixed-cost goods with extended longevity, which consumers typically intend to use for many years. Given Cisco's market dominance and the few alternatives available, end-users often have little choice in response to Cisco's price increases above a competitive level. In addition, end-users are disinclined to mix-and-match networking devices or make wholesale changes to their network environment, which can be cost-prohibitive.

26. As discussed further below, both the Ethernet switch and router markets have significant barriers to entry and are dominated by incumbents like Cisco—making it difficult (if not impossible) for new entrants to compete in the market.

II. CISCO'S MONOPOLY POWER IN THE RELEVANT PRODUCT MARKETS

27. Given its early entrance into the computer networking industry, Cisco has held a stranglehold on the supply of networking products in the United States for almost four decades, with a dominant market share that has reached 70% or more, including in the markets for routers and Ethernet switches. Given that both markets have high barriers to entry, Cisco faces little in the way of competition—just a handful of competing original equipment manufacturers ("OEM") supply the United States networking market, including Hewlett Packard Enterprise Company ("HPE"), Juniper Networks, Inc. ("Juniper"), Arista Networks Inc. ("Arista"), and Fortinet, Inc.[3] Yet, not one of these competing OEMs has ever cracked more than 20% of the relevant market share.

28. The sheer lack of competition within the networking industry has recently come under scrutiny, based on HPE's proposed $14 billion acquisition of Juniper. Earlier this year, the Antitrust Division of the United States Department

[3] *See* Cisco Systems, Inc., *SEC Form 10-K*, 6 (Sept. 5, 2024).

of Justice filed suit to block this merger, which would result in two companies—Cisco and HPE—controlling more than 70% of the U.S. market for wireless networking equipment. *See United States v. Hewlett Packard Enterprise Co.*, Case No. 5:25-cv-00951 (N.D. Cal.).

29. Given Cisco's early market entrance into the networking space—and, more specifically, in the manufacturing and servicing of Ethernet routers and switches—many networking environments use Cisco-branded routers and switches. Transitioning from Cisco Ethernet routers and switches to Ethernet routers and switches made by another OEM is expensive, requiring the replacement of significant hardware and the retraining of personnel. Given these market realities, Cisco networking customers are "captive customers" that are unable to turn to Ethernet routers and switches or other alternative technologies in response to a monopolist's price increase above the competitive level. As a result, Cisco is a monopolist in the Ethernet switch and router markets.

A. <u>The Relevant Switch Market.</u>

30. Ethernet switches are a relevant product market. The geographic markets for the sale of Ethernet switches are (i) the United States and (ii) the world. The global market for Ethernet switches includes manufacturers with product portfolios that are worldwide in scope and multinational customers that have a demand for such global capability. There is substantial industry recognition of

both a global market for Ethernet switches and a narrower U.S.-only market for Ethernet switches. A hypothetical monopolist of Ethernet switches in the United States would be able to raise prices profitably over competitive levels. Correspondingly, a hypothetical monopolist of Ethernet switches globally would be able to raise prices profitably over competitive levels. In fact, Cisco itself has been able to maintain prices above competitive levels both globally and in the United States.

31. Cisco has monopoly power in the United States and global markets for Ethernet switches, consistently holding shares above 50% in both markets, and is protected by high barriers to entry. Cisco's Ethernet switch market shares are commonly at least five times greater than the next Ethernet switch competitor in the United States, as well as commonly five times greater than the next Ethernet switch competitor globally. Cisco has managed to maintain its market dominance for almost thirty years, with global and U.S. market shares commonly exceeding 50%, and at times above 70%.

B. The Relevant Router Market.

32. The geographic markets for the sale of routers are (i) the United States and (ii) the world. The global market for routers includes manufacturers with product portfolios that are worldwide in scope and multinational customers that have a demand for such global capability. There is substantial industry

recognition of both a global market for routers and a narrower U.S.-only market for routers. A hypothetical monopolist of routers in the United States would be able to raise prices profitably over competitive levels. Correspondingly, a hypothetical monopolist of routers globally would be able to raise prices profitably over competitive levels. In fact, Cisco itself has been able to maintain prices for routers above competitive levels both globally and in the United States.

33. Cisco has monopoly power in the U.S. and global markets for routers, possessing in excess of 50% in both markets, and is protected by high barriers to entry. Cisco's router market shares are roughly at least five times greater than its closest router competitors in both the United States and global markets. Cisco has managed to maintain its market dominance on routers for almost thirty years, with global and U.S. market shares commonly exceeding 50%, and often above 70%.

C. The Barriers to Entry to the Relevant Product Markets.

34. The Relevant Router and Switch Markets are both characterized by high barriers to entry and expansion. Several factors contribute to these high entry and expansion barriers for potential new entrants and existing competitors. To begin with, the costs to develop router software and hardware as well as switch software and hardware are substantial, require tens of millions of dollars for initial development, and hundreds of millions more to tailor the product to specific customer needs and build an effective sales network.

35. Another barrier to entry for the Relevant Router and Switch Markets lies in customers' long purchase cycles when replacing or upgrading their network components to the next technology. These circumstances mean that competitors have limited opportunities to significantly expand their market share and take market share from competitors.

36. As Cisco publicly promotes,[4] it is the number one vendor for major network components often required by customers for their enterprise infrastructures—such as for wireless LAN and WAN equipment and telepresence products—in addition to Ethernet switches and routers. This, in turn, makes it even more difficult for Cisco end-users to switch from Cisco networking equipment to another competitor. In fact, changing to another networking manufacturer is cost-prohibitive (thereby presenting yet another barrier to entry), especially in light of the high transaction costs for customers and the presence of bundled offerings by Cisco.

37. To summarize, Cisco has monopoly power in the following Relevant Product Markets: the Relevant Switch Market (both globally and limited to the U.S.) and the Relevant Router Market (both globally and limited to the U.S.). Hereinafter, the Relevant Router and Switch Markets are referred to collectively

[4] *See* Patricia Costa, *Cisco ranked #1 (again!) in industrial networking*, Cisco Blogs (Aug. 13, 2020), available at https://blogs.cisco.com/industrial-iot/cisco-ranked-1-again-in-industrial-networking.

as the "Relevant Product Markets." Upon information and belief, Cisco may be engaging in the same coercive tactics with respect to other Product Markets, such as optics, access points, and network management software, which Summit 360 intends to fully probe in the course of this litigation.

III. CISCO VIEWS THE INDEPENDENT CHANNEL AS COMPETITION

38. Cisco uses contracted distributors and resellers to supply its networking equipment to end-users (the "Authorized Channel"). In doing so, Cisco places a multitude of restraints and requirements on these contracted resellers, including prohibiting them from purchasing excess supply that end-users no longer need and that could be resold at a discount to other customers on a limited budget.

39. Cisco sells networking equipment through one of two channels: the direct and indirect channel. As illustrated in Figure 2 below, through the "direct" channel, Cisco sells its equipment directly to end-users. In the "indirect" channel, equipment is sold either (i) from Authorized Channel partners directly to end-users (One-Tier) or (ii) from general distributors-to-Authorized Channel partners-to end-users (Two-Tier). Over the last two decades, Cisco has phased out the direct channel (which, upon information and belief, accounts for less than 10% of Cisco's revenue) in favor of the indirect channel. As of this filing, Cisco's Authorized Channel consists of more than 8,000 organizations in the United States.

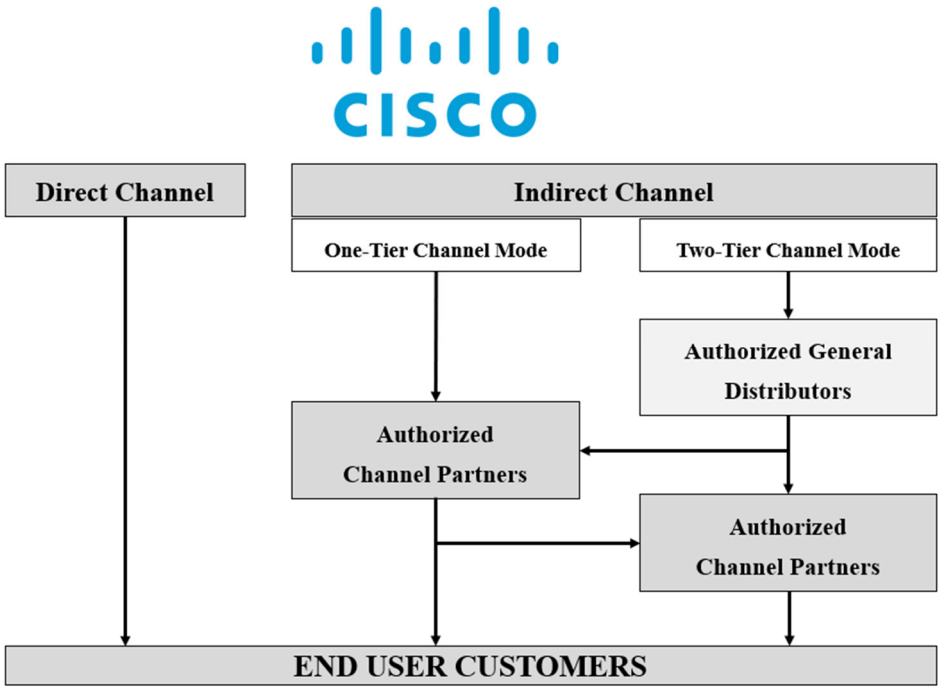

Figure 2

40. Depending on the distribution channel, Cisco mandates that Authorized Channel partners buy from certain distributors, and Cisco dictates the price and availability of Cisco's products vis-à-vis those distributors. These prices, in other words, reflect Cisco's monopoly pricing that it can impose on its distributors. The disparity in bargaining power between Cisco and its contracted resellers caused at least one court to hold Cisco's reseller agreement unconscionable.[5]

41. Under these circumstances, it is not surprising that the Independent Channel emerged. Upon information and belief, this channel generates billions of

[5] *See Infra-Comm Corp. v. Cisco Systems, Inc.*, 2008 WL 4925704 (Cal. Super. Oct. 27, 2008).

dollars in annual revenue that is not subject to Cisco's onerous restrictions and can offer support for customers that require networking equipment quickly and on a budget. The Authorized Channel cannot meet those customer requirements, but the Independent Channel can and, thus, provides a critical option for customers to meet their budget and timing requirements.

42. Rather than innovate its distribution system to meet customer demand, Cisco has treated the Independent Channel as an enemy and has instructed its sales force to do the same. As discussed below, Cisco arms its sales force with FUD tactics to employ if a customer considers the Independent Channel as a supply option.

43. Cisco's employees know that their FUD tactics scare their customers and enable Cisco to maintain its supra-competitive pricing. In fact, Cisco employees have celebrated when their FUD tactics successfully quash the Independent Channel and steer end-users back to the Authorized Channel.

44. Another reason Cisco treats the Independent Channel as an enemy is because independent resellers can sell Cisco's networking competitors' equipment without fear of consequence. Cisco's contracted resellers are incentivized to sell Cisco products, due to Cisco's expectations of volume, regardless of the customers' needs. Contracted resellers comply with Cisco's demands in an effort to avoid

adverse treatment by the monopolist, such as being terminated as an authorized reseller.

45. Rather than adapt to market needs, Cisco engages in a multi-faceted anticompetitive scheme intended to minimize or eliminate the Independent Channel, in an effort to re-capture the billions of dollars that Cisco loses to this channel, which not only harms independent resellers (like Summit 360), but also forces end-user customers to pay more.

IV. CISCO'S ANTICOMPETITIVE CONDUCT

A. Cisco's Abusive Brand Protection Practices.

46. Cisco has a designated global team—the "brand protection" team—that is responsible for identifying potential counterfeit products. According to Cisco, the stated purpose of its brand protection team is to combat illegal activities and protect Cisco's consumers.

47. In reality, Cisco uses brand protection as an extension of its sales team—to help facilitate more sales and maintain supra-competitive profits for Cisco. Indeed, assisting in Cisco sales is a key focus of Cisco's brand protection team, whose members routinely track transactions in which they successfully helped steer end-users from the Independent Channel to the Authorized Channel. Cisco's brand protection team accomplishes this in several ways, the most effective being the use of FUD tactics and customer-facing audits. In fact, Cisco's brand

protection team has gained a reputation in the networking industry as being aggressive and hostile towards Cisco's own customers and end-users.

48. Cisco's unlawful and anticompetitive practices directly impact Summit 360. Indeed, Summit 360's customers have encountered Cisco's anticompetitive tactics, which are illustrative of the general practices widely employed by Cisco and the anticompetitive harm that Summit 360 has suffered at the hands of Cisco. But because much of this information rests exclusively within Cisco's possession, Summit 360 expects that discovery will further establish the full extent of not only the harm to Summit 360, but also to the Independent Channel more generally.

i. Cisco's Use of FUD Tactics to Scare Customers from Purchasing from the Independent Channel.

49. Cisco uses various forms of FUD tactics to scare end-users from purchasing equipment from the Independent Channel. For Cisco employees, FUD is a flexible concept that's overall objective is to convey a message to its target (here, being the end-user) that ensures that the end-user ceases purchasing through the Independent Channel.

50. Cisco breeds a culture within its sales and brand protection teams that is hostile to the Independent Channel and to those that purchase from it. Cisco employees celebrate when they successfully divert end-users from the Indepdendent Channel to the Authorized Channel and are not shy to increasing

their hostility towards those that refuse to acquiesce. This is because sales representatives are, at least in part, compensated based on sales made in the Authorized Channel; however, when a transaction is made through the Independent Channel, they receive no commission or credit. Sales representatives, therefore, are naturally incentivized to ensure that end-users within their region or area purchase only through this channel.

51. In fact, to prevent a transaction with an independent reseller, Cisco's sales representatives have requested FUD material from the brand protection team to be shared with the end user. While characterized as "educational" in nature, Cisco's own employees know that the true purpose of these materials is to prevent end-users from purchasing through the Independent Channel, and Cisco employees use them to "scare" end-users from purchasing through the Independent Channel, which often has the intended result. As depicted in Figure 3 below, Cisco's FUD documents are directed at "small neighborhood businesses," among others, and aim to cast doubt as to the lower, more competitive, prices that

the Independent Channel offers:

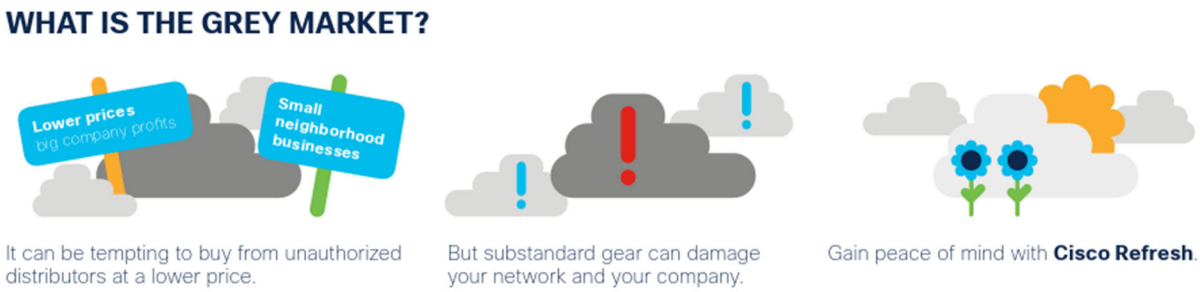

Figure 3

52. Indeed, Cisco's FUD tactics take various forms and approaches because its sales representatives have unfettered discretion on how to use them. In some cases, Cisco's sales representatives, with assistance from brand protection, prepare customer-facing documents that warn customers that their maintenance and service from Cisco will be at risk if they purchase from the Independent Channel. In other instances, Cisco's sales representatives have requested that brand protection draft language that sows FUD into an end-user about a specific independent reseller from whom it may be considering buying. Regardless of approach, the end goal is the same: to "scar[e] the sh*t out of" the end-user and to eradicate the Independent Channel.

53. Cisco's brand protection team is also asked by sales representatives to speak directly to end-users—in some cases, even before the end-user has made a purchase with an independent reseller.

54. For example, last year, Summit 360 was closing on a purchase order worth hundreds of thousands of dollars for Cisco hardware (namely, switches and routers) with a large cargo airline. While the parties were discussing the deal, but before the purchase was made, a Cisco sales representative (or one of its authorized resellers) told the airline that, among other things: (i) Summit 360 is not an authorized Cisco partner; (ii) dealing with Summit 360 could cause "security risks" to the airline; and (iii) Summit 360 was under "investigation" by Cisco. The timing was not a mere coincidence, but a clear attempt to interfere with a deal going to an independent reseller.

55. Upon information and belief, the timing of Cisco's "outreach" to end-users (including Summit 360 customers) is often intended to ensure that large projects—typically those worth hundreds of thousands to tens of millions of dollars—stay within the Authorized Channel.

56. Cisco's brand protection team also approaches end-users in an adversarial manner, often demanding documents and information relating to purchases with independent resellers. In this context, and given Cisco's monopoly in the Relevant Product Markets, end-users are left with no choice but to acquiesce, for fear of Cisco taking action against them. For example, when one Summit 360 customer was "looked at poorly by Cisco" for purchasing switches from Summit 360, it begrudgingly terminated its business relationship with Summit 360.

ii. Cisco's Customer Audits.

57. In addition to FUD, Cisco also uses audits to lock end-users into purchasing exclusively through Cisco's Authorized Channel. These audits, too, come in various forms—such as through Cisco's "free" customer "health check" or pursuant to End User License Agreements ("EULA"),[6] or Cisco's General Terms.[7]

58. For instance, Cisco offers a "complimentary" health check for end-users to verify, among other things, the authenticity of their products. Unbeknownst to end-users, however, is that by availing themselves to this service, they are inviting Cisco to examine their network and hardware for purposes of discovering "suspected" counterfeit products or products that were purchased outside Cisco's Authorized Channel. Often when this happens, Cisco becomes hostile toward the end-user—demanding from its own customer invoices and information regarding the at-issue products. To add insult to injury, when "unauthorized" products are found in an end-user's network, Cisco charges its

[6] *See* Cisco, *Cisco End User License Agreement*, available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/eula/eula-archived-eng-july-2022.pdf.

[7] *See* Cisco, *General Terms*, available at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/Cisco_General_Terms.pdf. According to Cisco's website, "Effective February 5, 2024, Cisco's End User License Agreement (EULA) has been replaced with Cisco's General Terms." *See* Cisco, *Cisco Contract Experience*, available at https://www.cisco.com/site/us/en/about/legal/contract-experience/index.html.

customers re-certification or re-licensing fees for each product—effectively punishing the customer for purchasing outside of the Authorized Channel.

59. For example, in 2023, Cisco performed a "product health check" for a Summit 360 customer, in which it determined that switches supplied by Summit 360 were "unauthorized" and "[s]uspected counterfeit." According to the end-user, Cisco "raked [them] over the coals for buying from a company that was not on their 'certified partner finder' list." While Cisco ultimately admitted that its counterfeit claims were not true, it still charged the end-user thousands of dollars to "re-license" the hardware supplied by Summit 360. The experience left the end-user unhappy with the increased costs and, since then, the end-user has not purchased equipment from Summit 360.

60. Similarly, a large furniture company stopped purchasing switches and routers from Summit 360 after Cisco began "billing [it] penalty costs for switches" supplied by Summit 360.

61. In addition to "health checks," Cisco has also exploited its EULAs and General Terms as a means for conducting audits of end-user network environments and to identify equipment supplied by the Independent Channel. Like most modern electronics, many Cisco products, including switches and routers, contain embedded software that is essential to the product's function and operation. Although consumers purchase the actual hardware (*e.g.*, switch or

router), Cisco has taken the position that the embedded software is licensed to its consumers through its EULA and General Terms. These agreements are simply click-through contracts that many end-users are entirely unaware of when they install and power up their networking equipment.

62. Unbeknownst to end-users, under both Cisco's EULA and General Terms, Cisco claims the right to audit customers to "verify" compliance. Not only are these audits a burden on the customer's day-to-day operations, but they are also costly. If Cisco determines that the customer has hardware from the Independent Channel, Cisco has demanded repayment for the cost of Cisco's audit, the cost of recertification, and the cost of replacing "non-compliant" products.

63. As part of its auditing process, Cisco demands royalties or other fees that it claims the customer owes for Cisco's purported IP rights. Cisco has demanded that customers pay for licenses on products that customers already purchased or to repay Cisco the cost of having to recertify the hardware.

64. These audits and demands for license royalty payments are part of Cisco's anticompetitive scheme to eliminate or minimize the Independent Channel. Through these audits, Cisco has been able to secure agreements with end-users not to purchase from the Independent Channel. As deployed by Cisco, these audits and license demands are not designed to protect customers; on the

contrary, they are intended to generate greater sales opportunities, while seeking to eliminate the Independent Channel. In doing so, Cisco's audits and demands only buttress the harmful effects of Cisco's overall course of conduct.

65. For instance, Summit 360 has a long-standing relationship with a publicly traded freight operations company and, historically, has supplied this end user various networking products, including switches and routers. Last year, the end-user anticipated placing a large, seven-figure, order for switches. Upon information and belief, due to pressure and threats received from Cisco, the end-user no longer purchases new switches or routers from Summit 360, and Summit 360 was unable to participate in the seven-figure bid.

iii. Cisco's Restrictive IOS Update Policies and Recertification Costs.

66. Customers of networking equipment require maintenance, service, and IOS updates to ensure the proper functioning of their equipment. Only Cisco can provide comprehensive maintenance and software support on its router and Ethernet switch products. These maintenance services include onsite visits from certified engineers, software updates, technical assistance center ("TAC") access, online resources, and hardware replacement services (collectively, "Maintenance Services"). Without such Maintenance Services, customers may not be able to address critical performance issues and service problems that impact their businesses.

67. Customers that are unable to afford Maintenance Services provided by Cisco rely on third-party maintenance and service providers to provide hardware maintenance and support; however, due to Cisco's policies, these third-party providers cannot always offer software maintenance and support. Thus, Cisco is able to maintain a price premium for its Maintenance Services, including its service packages offered under the brand names SmartNet, DNA, and Catalyst.

68. Since Charles Robbins took over as Chief Executive Officer of Cisco in 2015, the company has made a concerted effort to evolve from a hardware company to a software company. In an interview with *Fortune*, Mr. Robbins discussed his goals as Cisco's new CEO, including the strategic decision to focus on software for its networking equipment and to generate greater revenue from its subscription-based products.[8] Eight years later, Cisco boasted a "double-digit growth in subscription and software revenues."[9]

69. Much of Cisco's continued growth is due to its anticompetitive maintenance practices in which only Cisco and Cisco-authorized dealers are allowed to repair Cisco hardware or update Cisco software. Cisco maintenance services are offered through, among other things, its SmartNet service package

[8] Adam Lashinsky, *Cisco CEO Chuck Robbins is flipping all the right switches*, Fortune (Aug. 25, 2015), available at https://fortune.com/2015/08/26/cisco-ceo-chuck-robbins-changes/.
[9] Joseph F. Kovar, *Cisco CEO Sees Growth From Security, Software, Generative AI*, The Channel Co. (May 17, 2023), available at https://www.crn.com/news/security/cisco-ceo-chuck-robbins-raising-our-fiscal-2023-outlook.

and through its suite of licensing subscription packages. Because Cisco's hardware operates on proprietary IOS software that is essential to the product's function and operation, many end-users feel compelled to purchase service contracts and subscription packages, to ensure IOS updates remain available. Indeed, as Cisco itself acknowledges, "[w]ithout [software] updates or upgrades, the functionality of the software would diminish over a relatively short time period."[10]

70. And while many of Cisco's new generation of switches offer IOS updates without SmartNet, they still require a licensing subscription and a Smart Account associated with the hardware in order to obtain essential IOS updates.

71. Historically, end-users have been able to purchase Cisco switches and routers through the Independent Channel and receive the necessary support and/or services when needed. Upon information and belief, when Cisco first began embedding software into its networking hardware, it made IOS updates available regardless of the channel in which the end-user purchased equipment. Beginning in or around 2009, however, Cisco developed new policies intended to limit the availability of IOS updates to only the original end-user. Even still, these updates were available to end-users that purchased switches and routers through the Independent Channel by, among other things, purchasing SmartNet. In

[10] *See* Cisco Systems, Inc., *SEC Form 10-K*, 67 (Sept. 5, 2024).

addition, Cisco's earlier models of switches and routers did not require a software license.[11]

72. More recently, Cisco has rolled out a new "smart" licensing policy and program for its new model of switches and routers. Unlike prior generations, Cisco's new fleet of networking equipment requires a software subscription as part of the purchase of any new switches or routers and limits IOS updates to original end-users. These subscriptions are offered in two different tiers (Essentials and Advantage) and provide similar services available under SmartNet: software support, TAC services, and return material authorization options, among others.

73. These new policies and programs mark the latest attempt by Cisco to eliminate competition with the Independent Channel and maintain even greater market power and control. As intended, independent resellers like Summit 360 cannot supply newer models of switches and routers with the subscriptions necessary for end-users to obtain key software updates. This is by design: it effectively boxes out independent resellers from competing in the Relevant Product Markets. And it has worked, as Summit 360 has lost several customers

[11] *See* Cisco, *Cisco Catalyst 2960-X Series FAQ* (Feb. 26, 2018), available at https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/qa_c67-728348.html.

because they are not able to obtain these new subscription packages and updates through Summit 360.

74. In addition, to the extent that independent resellers are able to procure and supply equipment for end-users, Cisco has a long-standing re-certification policy that is intended to increase the costs for end-users such that they do not repurchase from the Independent Channel in the future. For instance, when end-users purchase equipment from independent resellers and seek support or assistance with Cisco—including to have equipment covered by a SmartNet contract—they are charged a "re-certification" fee. These expenses, however, can be more than the value of the equipment itself and, effectively, leave the end-user with no option other than to purchase entirely new equipment. Worse yet, these recertification costs are typically a black box, with no explanation provided by Cisco as to how it determines the fees charged to the end-user.

75. But these practices have their intended effect: steering customers away from the Independent Channel back into the Authorized Channel. For example, Cisco offered to "recertify" switches previously supplied by Summit 360 to a school district. However, because the recertification costs were more than the actual value of the hardware, the school district had no choice but to purchase brand new switches from an authorized reseller.

76. Despite all of this, given the high cost of purchasing new equipment from other OEMs, coupled with a preference towards utilizing a familiar name brand in Cisco, end-users are effectively locked-in to purchasing from Cisco. If end-users are faced with an increase in price for service contracts, software updates, or subscription packages, they will continue to pay supra-competitive prices rather than purchase new networking equipment from a competing OEM.

77. These measures and policies serve no valid business purpose and are intended to eliminate Cisco's competition with the Independent Channel. Indeed, the Department of Justice has expressly called out these draconian licensing practices as leading end-users to experience "Cisco fatigue."[12] Prohibiting end-users from getting key IOS updates if they do not buy within the Authorized Channel makes sense only because it is designed to eliminate the Independent Channel and to force end-users to purchase through the Authorized Channel, where Cisco is able to maintain supra-competitive prices.

B. Cisco's Counterfeit Problem.

78. Cisco has contract manufacturers all around the world that are responsible for, among other things, manufacturing network switches and routers. A significant portion of Cisco's switches and routers are manufactured in the

[12] *See United States v. Hewlett Packard Enterprise Co.,* Case No. 5:25-cv-00951, ECF No. 1, at ¶ 37 (N.D. Cal., Jan. 30, 2025).

Asian-Pacific region and, more specifically, China. Upon information and belief, several of Cisco's Chinese contract manufacturers have been tied to the manufacturing of counterfeit Cisco-branded products—many of which are sold in both the Authorized and Independent Channels.

79. These counterfeit products are not akin to counterfeit name-brand goods one might come across on Canal Street in New York City; on the contrary, these counterfeit Cisco-branded products appear and function like the authentic product.

80. According to Cisco, a "counterfeit" product can be anything from a product that was manufactured by a counterfeit manufacturer, to a product manufactured by a contract manufacturer without Cisco's authorization, to a product that had parts replaced, to a product that received an upgrade. Cisco's counterfeit determinations are largely based on a comparison of the product's serial numbers against Cisco's manufacturing records, which are not available to the public. Using this analysis, Cisco categorizes *potential* counterfeits based on perceived risk (ranging from "High Risk" to "Low Risk").

81. Many of these purported counterfeit products are manufactured in China in close proximity with Cisco's authorized contract manufacturers. These products are then exported from China to the United States and sold, both in the Authorized and Independent Channels, to domestic end-users.

82. For example, an extensive and elaborate network of counterfeit manufacturing plants has been established throughout China. Upon information and belief, these counterfeit factories use similar (if not the same) tools and resources to manufacture Cisco-branded products and, on occasion, have worked with Cisco's authorized contract manufacturers. In many cases, these counterfeit Cisco-branded products are indistinguishable from legitimate Cisco-authorized products and operate just as well.

83. Cisco posts purported instructions on its website for end-users to identify potential counterfeit products. These instructions focus on security labels on the product's packaging, chassis, and circuit boards. However, given the simplicity of replicating these labels, Cisco's instructions are of minimal use for end-users and resellers (even contracted resellers), alike, to identify potential counterfeit.

84. Like other networking manufacturers, Cisco has also developed various tools that purportedly identify counterfeit products—including a packaging verification tool that Cisco claims allows it to screen products to determine product authenticity within seconds. However, unlike these other networking manufacturers, Cisco's tools are not readily available to the public—thereby depriving end-users and resellers of the ability of independently verifying

a product's authenticity or challenging Cisco's counterfeit determination. This is intentional.

85. In fact, rather than solve this issue, Cisco leverages its counterfeit problem as a way of scaring customers who seek to procure products through the Independent Channel. For instance, Cisco has not hesitated to claim to end-users that their hardware may be counterfeit or is "suspected" counterfeit—despite not having even physically inspected the product. Worse yet, these "suspected" counterfeit determinations are not accurate and, as discussed above, Cisco has had to withdraw these initial findings after completing a more comprehensive assessment. At that point, however, the intended harm has already been done.

86. Given Cisco's monopolies in the Relevant Product Markets, and end-users' inability to challenge Cisco's claims, it is a no-win situation for consumers. Upon information and belief, Cisco refuses to change its manufacturing practices because it seeks to "win" on both ends: take advantage of the lower manufacturing costs in China and, at the same time, use purported counterfeit to its advantage to shut down its most potent competitive threat in the United States— the Independent Channel.

C. Cisco Knows Its Conduct Is Illegal.

87. This is not the first time Cisco has been called out for its anticompetitive conduct. One of Cisco's networking competitors previously

brought an antitrust case against Cisco because Cisco was using its IP litigation against a competitor as a FUD tactic to dissuade customers from making purchases with the competitor.

88. In that case, Cisco argued that its IP-based litigation was immunized by the *Noerr-Pennington* doctrine. The court rejected that argument, holding that there was ample evidence to support that Cisco's coercive statements to customers were not incidental to its IP litigation.[13] Rather, Cisco's statements to customers were designed to dissuade competitive purchases, not merely to maintain its purported IP rights. The court further found on summary judgment that Cisco's FUD tactics constitute anticompetitive conduct and that Cisco's IP litigation could be found to be part of that anticompetitive scheme. As a result, the court ruled that there was sufficient evidence to find that Cisco is a monopolist that abused its power to foreclose competition.

89. More recently, another federal court found on summary judgment that a similar variant of Cisco's FUD tactics could also constitute an antitrust violation.[14] In that case, brought by an independent reseller, the reseller explained that Cisco created FUD through its brand protection and other coercive practices, similar to those discussed above. There, Cisco repeated similar arguments made

[13] *See Arista Networks, Inc. v. Cisco Sys. Inc.*, 2018 WL 11230167 (N.D. Cal. May 21, 2018).
[14] *See Dexon Computers Inc. v. Cisco Sys. Inc.*, 2024 WL 180775 (E.D. Tex. Jan. 17, 2024).

in its prior antitrust case, which the court rejected in the same fashion. At trial, Cisco employees were called to the stand in an attempt to downplay their use of FUD tactics.

90. Rather than learn from these experiences, Cisco has proven to be a recidivist. It refuses to stop using FUD, coercion, technological barriers, and associated legal threats so long as it achieves its anticompetitive objectives. Namely, Cisco has engaged in an overall course of conduct to eradicate or otherwise minimize interbrand and intrabrand competition from the Independent Channel. Upon information and belief, Cisco does not care about the reputational ramifications of its conduct, so long as it maintains its monopoly in the Relevant Product Markets.

91. With billions of dollars' worth of Ethernet switches and routers sold each year in the Independent Channel, there is a substantial amount of commerce involved within the Relevant Product Markets for which Cisco is abusing its monopoly power to recapture.

V. CISCO'S ANTICOMPETITIVE CONDUCT HARMS COMPETITION

92. Cisco's anticompetitive conduct is intended to—and does—force customers to access networking equipment exclusively through the most expensive contracted channel, while foreclosing Cisco's equipment competitors from making sales to end-users. Cisco was not always hostile to the Independent

Channel. On the contrary, the Independent Channel has benefited Cisco by offering customers more affordable options on networking equipment, which has improved Cisco's installed base and has assisted Cisco in becoming the most popular networking equipment provider. Despite this, Cisco has now pivoted to targeting and eradicating this channel, in an effort to increase its prices and further pad its $21.4 billion profit margins to the detriment of the Independent Channel and Cisco's end-users.

93. The inevitable effect of this course of conduct is to drive supra-competitive prices in the Relevant Product Markets and prevent customers from finding alternatives. While, in theory, customers could divert purchases in the Relevant Product Markets to Cisco's competitors, the reality is that Cisco's installed base of equipment is a large portion of its customers' respective networks, making it financially and logistically impossible for many customers to make a wholesale change, or to even do so over an extended period of time.

94. Because of Cisco's monopoly power, many customers have no choice but to purchase overpriced equipment in the Relevant Product Markets on Cisco's terms or face coercion and retribution from Cisco in the form of, among other things, disruptive and costly audits, expensive hardware recertifications, suspended services and support, unavailable software updates, and even threatened legal action.

95. And Cisco's brand protection practices are not reasonably necessary to achieve any cognizable procompetitive benefit. On the contrary, the harm from these practices outweighs any procompetitive benefits, which could be achieved through less restrictive means.

VI. SUMMIT 360 HAS SUFFERED AN ANTITRUST INJURY

96. Cisco's overall course of conduct is specifically designed to foreclose or otherwise eliminate the Independent Channel through which customers can (i) purchase equipment from manufacturers that compete with Cisco and (ii) secure Cisco products for a lower price. Summit 360's injury flows from Cisco's efforts to raise prices, reduce quality, lower output, and eliminate competition. Summit 360 has lost customers, sales, revenues, and profits due to the anticompetitive and coercive tactics employed by Cisco.

97. In one example, Cisco claimed to a customer that it was investigating Summit 360 for purported counterfeit, when Cisco itself had approved the SmartNet service package the customer had purchased associated with the equipment. Cisco's SmartNet approval process requires identification of the equipment to which the SmartNet would apply, and with that information, upon information and belief, Cisco approved the service agreement. Cisco would not approve a SmartNet service package if it had any reason to doubt the origin of the

products to which the service contract would apply. As a result of Cisco's anticompetitive tactics, Summit 360 lost this end-user as a customer.

98. As a further example, Summit 360 lost another customer because Cisco told the customer that if it purchased switches or routers from the Independent Channel, Cisco would continue to impose financial penalties.

99. Cisco's conduct is designed to harm resellers like Summit 360 precisely because of the benefits that it (like others within the Independent Channel) has provided for decades, which run counter to Cisco's profit motives. Cisco is a classic monopolist that knows that it can earn more profit by limiting supply and forcing customers into more expensive, contracted channels than by competing with the Independent Channel. If Cisco can force end-users to purchase from contracted channels, then Cisco's preferred dealers do not need to negotiate for price reductions or quality improvements that would impact Cisco's bottom line. The coercion, deception, technological barriers, and other anticompetitive conduct at issue in this case allows Cisco to maintain—and even grow—its monopoly power, and Summit 360's losses are a direct byproduct of this anticompetitive conduct.

100. Like other independent resellers, Summit 360 has also sustained losses to its goodwill and reputation in the networking industry by virtue of Cisco's anticompetitive conduct. Cisco's monopoly in the Relevant Product

Markets makes it immune to customer dissatisfaction and allows it to blame Summit 360 and other independent resellers. Namely, rather than respond to customer feedback and attempt to win purchases by virtue of competition on the merits (*i.e.*, offering better prices, quality, or service), Cisco has attempted to portray Summit 360 as an unworthy sales partner who causes the customers' problems. But this is not the case, as Summit 360 has spent decades building trust and goodwill with its customers, even to the benefit of Cisco. Now that Cisco's priority is to eliminate a channel that would lower its prices, Summit 360 is being painted in a negative light in an attempt to drive it out of business.

COUNT I
Unlawful Monopolization of the Relevant Product Markets Under Section 2 of the Sherman Act

101. Summit 360 repeats and realleges each of the allegations set forth in the preceding paragraphs as if fully set forth herein.

102. At all times relevant, Cisco has had monopoly power in the United States in each of the Relevant Product Markets.

103. Cisco's conduct constitutes the intentional and unlawful maintenance of monopoly power in each of the Relevant Product Markets, in violation of Section 2 of the Sherman Act, 15 U.S.C. § 2.

104. For the purpose of maintaining its monopoly power, Cisco committed numerous acts, including:

a. Engaging in FUD and associated coercive tactics pursuant to its overall goal to force supra-competitive purchases through Cisco's Authorized Channel;

b. Engaging in customer audits designed to stunt overall competition in the Relevant Product Markets and likely other markets;

c. Imposing unreasonable and exclusionary technological barriers that, among other things, block access to IOS updates to equipment supplied through the Independent Channel; and

d. Taking advantage of its own counterfeiting problem to eliminate or minimize the competitive threat the Independent Channel poses.

105. These measures serve no valid business purpose and are imposed for purposes of eliminating competition in the Relevant Product Markets.

106. Cisco's conduct has injured competition in the Relevant Product Markets, suppressed Summit 360's sales in those markets and the products of other competitors, diminished Summit 360's future sales opportunities, and increased Summit 360's operating costs.

107. Cisco's conduct has and will continue to maintain supra-competitive prices to customers in the Relevant Product Markets, harm innovation associated

with the products offered in the Relevant Product Markets, and otherwise deprive customers of their ability to make an unfettered choice of technology on the merits.

COUNT II
Unlawful Attempted Monopolization of the Relevant Product Markets in Violation of Section 2 of the Sherman Act

108. Summit 360 repeats and realleges each of the allegations set forth in the preceding paragraphs as if fully set forth herein.

109. Cisco acted with a specific intent to monopolize and destroy competition in the Relevant Product Markets. Cisco devised and implemented an overall plan to force customers to pay supra-competitive prices in the Relevant Product Markets, with the associated destruction of competition in the Relevant Product Markets.

110. Cisco willfully engaged in a course of anticompetitive conduct to obtain a monopoly in the Relevant Product Markets, including:

a. Engaging in FUD and associated coercive tactics pursuant to its overall goal to force supra-competitive purchases through Cisco's Authorized Channel;

b. Engaging in customer audits designed to stunt overall competition in the Relevant Product Markets and likely other markets;

c. Imposing unreasonable and exclusionary technological barriers that, among other things, block access to IOS updates to equipment supplied through the Independent Channel; and

d. Taking advantage of its own counterfeiting problem to eliminate or minimize the competitive threat the Independent Channel poses.

111. These measures serve no valid business purpose and are imposed for purposes of eliminating competition in the Relevant Product Markets.

112. Throughout the time Cisco engaged in this anticompetitive conduct, it had a dangerous probability of succeeding in gaining a monopoly in and controlling each of the Relevant Product Markets and continuing to maintain supra-competitive prices and exclude its competitors.

113. Cisco's conduct has injured competition in the Relevant Product Markets, suppressed Summit 360's sales in those markets and the products of other competitors, diminished Summit 360's future sales opportunities, and increased Summit 360's operating costs.

114. Cisco's conduct has and will continue to maintain supra-competitive prices to customers in the Relevant Product Markets, harm innovation associated with the products offered in the Relevant Product Markets, and otherwise deprive customers of their ability to make an unfettered choice of technology on the merits.

COUNT III
Violation of the Minnesota Antitrust Law

115. Summit 360 repeats and realleges each of the allegations set forth in the preceding paragraphs as if fully set forth herein.

116. Cisco acted with a specific intent to monopolize and destroy competition in the Relevant Product Markets in violation of Minnesota Statutes section 325D.52. Cisco devised and implemented an overall plan to force customers to pay supra-competitive prices in the Relevant Product Markets, with the associated destruction of competition in the Relevant Product Markets.

117. Cisco willfully engaged in a course of anticompetitive conduct to obtain and maintain a monopoly in the Relevant Product Markets, including:

a. Engaging in FUD and associated coercive tactics pursuant to its overall goal to force supra-competitive purchases through Cisco's Authorized Channel;

b. Upon information and belief, engaging in customer audits designed to stunt overall competition in the Relevant Product Markets and likely other markets;

c. Imposing unreasonable and exclusionary technological barriers that, among other things, block access to IOS updates to equipment supplied through the Independent Channel; and

d. Taking advantage of its own counterfeiting problem to eliminate or minimize the competitive threat the Independent Channel poses.

118. These measures serve no valid business purpose and are imposed for purposes of eliminating competition in the Relevant Product Markets.

119. Throughout the time Cisco engaged in this anticompetitive conduct, it has had monopoly power in the United States in each of the Relevant Product Markets or, alternatively, has had a dangerous probability of succeeding in gaining a monopoly in and controlling each of the Relevant Product Markets and continuing to maintain supra-competitive prices and exclude its competitors.

120. Cisco's conduct has injured competition in the Relevant Product Markets, suppressed Summit 360's sales in those markets and the products of other competitors, diminished Summit 360's future sales opportunities, and increased Summit 360's operating costs.

121. Cisco's conduct has and will continue to maintain supra-competitive prices to customers in the Relevant Product Markets, harm innovation associated with the products offered in the Relevant Product Markets, and otherwise deprive customers of their ability to make an unfettered choice of technology on the merits.

COUNT IV
Tortious Interference with Prospective Economic Advantage

122. Summit 360 repeats and realleges each of the allegations set forth in the preceding paragraphs as if fully set forth herein.

123. Summit 360 had a reasonable expectation of economic advantages in the form of ongoing sales of Cisco switches and routers to established and regular Cisco end-users.

124. Cisco was well-aware of independent resellers, including Summit 360, and their expectation of sales to end-users.

125. Cisco has intentionally sought—and continues to seek—to reduce and eliminate sales through the Independent Channel by deploying various, independent, tortious acts, including acts in contravention with Section 2 of the Sherman Act.

126. In the absence of Cisco's intentional interference, Summit 360 would have continued making substantial sales to end-users.

127. As a direct and proximate result of Cisco's intentional interference, Summit has suffered damages, including the loss of sales and of goodwill.

128. To the extent compensable, Summit 360 is entitled to receive compensation for the pecuniary harm caused by Cisco.

129. If Cisco is allowed to continue engaging in the conduct, practices, and activities described herein, and unless adequate relief is afforded to Summit 360

so as to enjoin Cisco from engaging in such conduct, Summit 360 will be subjected to irreparable harm for which it has no adequate remedy at law.

PRAYER FOR RELIEF

Summit 360, Inc. prays for judgment and relief against Cisco as follows:

a. An Order directing the termination of all anticompetitive conduct in violation of Section 2 of the Sherman Act (15 U.S.C. § 2) and the Minnesota Antitrust Law, Minn. Stat. § 325D.52;

b. Treble damages (including lost profits), in an amount to be determined at trial and that cannot now be adequately quantified before relevant discovery;

d. Awarding Summit 360's costs of suit herein, including its attorneys' fees incurred in asserting antitrust claims;

i. An award of punitive damages in an amount sufficient to punish Cisco, to make an example of it to the community, and to deter Cisco from such conduct as to Summit 360 or others in the future;

j. For equitable remedial efforts by Cisco sufficient to rehabilitate Summit 360's damaged reputation;

k. For orders restraining Cisco from engaging in similar conduct in the future; and

p. Such other and further relief as this Court deems just and equitable.

DEMAND FOR JURY TRIAL

Summit 360 demands a trial by jury on all issues so triable.

Dated: May 22, 2025
Minneapolis, MN

Respectfully submitted,

ROBINS KAPLAN LLP

By: */s/Stephen P. Safranski*

Stephen P. Safranski (#0331326)
Eric P. Barstad (#0398979)
800 LaSalle Avenue
Suite 2800
Minneapolis, MN 55402
SSafranski@RobinsKaplan.com
EBarstad@RobinsKaplan.com
Phone: (612) 349-8500

MANATT, PHELPS, & PHILLIPS LLP

Matthew F. Bruno (*pro hac vice* forthcoming)
7 Times Square
New York, NY 10036
MBruno@manatt.com
Phone: (212) 790-4525

Dylan Carson (*pro hac vice* forthcoming)
1050 Connecticut Avenue, NW
Suite 600
Washington, DC 20036
DCarson@manatt.com
Phone: (202) 585-6600

Amar L. Thakur (*pro hac vice* forthcoming)
12730 High Bluff Dr.
Suite 300

San Diego, CA 92130
AThakur@manatt.com
Phone: (619) 205-5800

Rebecca Finkel (*pro hac vice* forthcoming)
151 N. Franklin St.
Suite 2600
Chicago, IL 60606
RFinkel@manatt.com
Phone: (312) 529-6300

Attorneys for Plaintiff Summit 360, Inc.